Esercitazione sull'utilizzo di nmap

Eseguire i seguenti tipi di scan sulla macchina metasploitable:

1. **Scansione TCP**
2. **Scansione Syn**
3. **Scansione con nmap -A**

Evidenziare le differenze tra la scansione TCP e la scansione SYN intercettando le richieste con Wireshark.

1- Scansione TCP

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-28 16:31 EST
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:BB:64:B5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
```

12	13.460223046	192.168.50.100	192.168.50.101	TCP	58 57261 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	13.460347143	192.168.50.100	192.168.50.101	TCP	58 57261 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	13.460389954	192.168.50.100	192.168.50.101	TCP	58 57261 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	13.460432026	192.168.50.100	192.168.50.101	TCP	58 57261 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	13.460624316	192.168.50.100	192.168.50.101	TCP	58 57261 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	13.460673826	192.168.50.100	192.168.50.101	TCP	58 57261 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	13.460713709	192.168.50.100	192.168.50.101	TCP	58 57261 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	13.460984830	192.168.50.100	192.168.50.101	TCP	58 57261 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	13.461396834	192.168.50.101	192.168.50.100	TCP	60 80 → 57261 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
21	13.461400340	192.168.50.101	192.168.50.100	TCP	60 25 → 57261 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
22	13.461400530	192.168.50.101	192.168.50.100	TCP	60 256 → 57261 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	13.461400704	192.168.50.101	192.168.50.100	TCP	60 445 → 57261 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
24	13.461400873	192.168.50.101	192.168.50.100	TCP	60 995 → 57261 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	13.461401048	192.168.50.101	192.168.50.100	TCP	60 22 → 57261 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
26	13.461401217	192.168.50.101	192.168.50.100	TCP	60 139 → 57261 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
27	13.461477693	192.168.50.100	192.168.50.101	TCP	54 57261 → 80 [RST] Seq=1 Win=0 Len=0
28	13.461542377	192.168.50.100	192.168.50.101	TCP	54 57261 → 25 [RST] Seq=1 Win=0 Len=0
29	13.461583663	192.168.50.100	192.168.50.101	TCP	54 57261 → 445 [RST] Seq=1 Win=0 Len=0
30	13.461632839	192.168.50.100	192.168.50.101	TCP	54 57261 → 22 [RST] Seq=1 Win=0 Len=0
31	13.461674365	192.168.50.100	192.168.50.101	TCP	54 57261 → 139 [RST] Seq=1 Win=0 Len=0
32	13.462054541	192.168.50.101	192.168.50.100	TCP	60 53 → 57261 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
33	13.462088525	192.168.50.100	192.168.50.101	TCP	54 57261 → 53 [RST] Seq=1 Win=0 Len=0
34	13.462180795	192.168.50.100	192.168.50.101	TCP	58 57261 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

2- Scansione SYN

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-28 16:56 EST
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:BB:64:B5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
20	13.180204459	192.168.50.100	192.168.50.101	TCP	74	44124 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1984370028 TSecr=0 WS=128
21	13.180275241	192.168.50.100	192.168.50.101	TCP	66	40340 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370028 TSecr=163931
22	13.180483658	192.168.50.100	192.168.50.101	TCP	74	53124 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1984370029 TSecr=0 WS=128
23	13.180645992	192.168.50.101	192.168.50.100	TCP	74	21 → 52920 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=163931 TSecr=1984370027 WS=32
24	13.180646718	192.168.50.101	192.168.50.100	TCP	74	80 → 38772 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=163931 TSecr=1984370028 WS=32
25	13.180664597	192.168.50.100	192.168.50.101	TCP	74	48530 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1984370029 TSecr=0 WS=128
26	13.180728219	192.168.50.100	192.168.50.101	TCP	66	52920 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370029 TSecr=163931
27	13.180762459	192.168.50.100	192.168.50.101	TCP	66	38772 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370029 TSecr=163931
28	13.180921271	192.168.50.100	192.168.50.101	TCP	74	37696 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1984370029 TSecr=0 WS=128
29	13.181070644	192.168.50.101	192.168.50.100	TCP	60	993 → 33706 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	13.181071283	192.168.50.101	192.168.50.100	TCP	60	587 → 60052 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	13.181071518	192.168.50.101	192.168.50.100	TCP	74	111 → 44124 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=163931 TSecr=1984370028 WS=32
32	13.181101665	192.168.50.100	192.168.50.101	TCP	66	40340 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370029 TSecr=163931
33	13.181161908	192.168.50.100	192.168.50.101	TCP	66	44124 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370029 TSecr=163931
34	13.181332927	192.168.50.100	192.168.50.101	TCP	66	52920 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370029 TSecr=163931
35	13.181446654	192.168.50.100	192.168.50.101	TCP	66	38772 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370030 TSecr=163931
36	13.181643599	192.168.50.100	192.168.50.101	TCP	66	44124 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370030 TSecr=163931
37	13.181653778	192.168.50.101	192.168.50.100	TCP	60	135 → 53124 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	13.181654369	192.168.50.101	192.168.50.100	TCP	74	22 → 48530 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=163931 TSecr=1984370029 WS=32
39	13.181654585	192.168.50.101	192.168.50.100	TCP	74	23 → 37696 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=163931 TSecr=1984370029 WS=32
40	13.181753677	192.168.50.100	192.168.50.101	TCP	66	48530 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370030 TSecr=163931
41	13.181813948	192.168.50.100	192.168.50.101	TCP	66	37696 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370030 TSecr=163931
42	13.181865357	192.168.50.100	192.168.50.101	TCP	66	48530 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370030 TSecr=163931
43	13.181914493	192.168.50.100	192.168.50.101	TCP	66	37696 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1984370030 TSecr=163931

3- nmap -A

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.50.101 -p 1-1024
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-28 17:01 EST
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      44119/tcp   mountd
|   100005  1,2,3      48107/udp   mountd
|   100021  1,3,4      37104/tcp   nlockmgr
|   100021  1,3,4      48822/udp   nlockmgr
|   100024  1          38940/tcp   status
|_  100024  1          39089/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open              Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

```
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:BB:64:B5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-12-28T17:02:43-05:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h30m09s, deviation: 3h32m17s, median: 2s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   1.01 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.67 seconds
```